NAC REPORTS

NAVAL ASSOCIATION OF CANADA
ASSOCIATION NAVALE DU CANADA

Conference Report on "Stickhandling Through Roughing and Interference: How to Position Canada in the Great Power Plays"

Dr. Ann Griffiths

In this report, I would like to summarize and reflect on the conference hosted by the Conference of Defence Associations in Ottawa in early March 2020. It's always challenging to sum up the discussion at a conference. There are multiple panels with multiple speakers on different topics. The speakers are allotted a certain amount of time, and thus must keep their presentations focused. This means that due to scheduling, some things get discussed and other things do not. In theory we could assume that what gets discussed is important, and what does not get discussed is not. In reality that may not be the case.

Let me start by saying that the conference was interesting and engaging. It was entitled "Stickhandling Through Roughing and Interference: How to Position Canada in the Great Power Plays." While catchy, and much appreciated by hockey fans, the conference did not really focus on this. The title suggests that there would be a discussion of how Canada can position itself in a world where the great powers are pulling it in different directions. It would have been useful to look more closely at Canada, and how Canadian national interests are affected by great powers, how Canada fits into a newly uncertain world, and the challenges for Canada that come with the changed geopolitical world. As this report will illustrate, the discussion took a very different direction. The organizers should perhaps have decided on one option – the first part of the title and a focus on great power roughing and interference, or how Canada can stickhandle through it.

The opening remarks asked difficult questions. What will security and defence look like in 10 years? What will soldiers (and presumably sailors and air force personnel too) be like in 10 years? How will militaries recruit their personnel? What equipment will militaries use and what digital threats will need to be countered? These were the focus of the conference rather than positioning Canada in a great power play.

This year started with a bang and has continued to deliver security challenges. The challenges we've seen thus far in 2020 are all non-traditional but nonetheless can involve, and have involved, military personnel. In just the first months of this year, there have been fires, floods, snowstorms and now COVID-19. The challenges associated with climate change continue, as does the threat from non-state actors. The list of roles that militaries must play gets longer as issues are added and none are subtracted.

The first panel discussed relations with Russia. It became clear from the discussion that Russia is seen as a challenge, but not in the way it was during the Cold War. One panelist called for treaties that were signed during the Cold War to be updated, rather than abandoned, and for them to include technology and new forms of conflict. Treaties are designed to increase confidence in interactions, so the fact that Russia is breaking or abandoning treaties – as is the United States – is an indication of a lack of confidence in state interactions. It is not enough, however, to update treaties, they have to be enforced as well.

Russia has been focusing on new weapons and new military materiel even as its economy deteriorates. But although it is developing new military weapons, it represents a greater threat perhaps in its ability and willingness to use hybrid warfare and hybrid activity to destabilize the West. It may not invade the West, but it is dividing, destabilizing and distracting. And as the West squabbles, Russia hopes to reclaim chunks of territory that it considers its own.

A speaker from Latvia provided the perspective of a state in the shadow of Russia. He noted that Latvia has experienced interference from Russia and is subjected to false information on a daily basis. It has learned that information has to be monitored constantly and countered immediately. Russia has discovered the weaknesses in the West and works to exploit them as it attempts to regain its status as a global power. It exploits weakness not necessarily by military invasion, although it has of course done that, but by disinformation, information manipulation and cyber-attacks. The way to protect the West from Russia's malign activities is to stand together to support democratic principles and way of life. But unfortunately the West has been reactive – it simply reacts when Russia acts – and this is a losing strategy when it comes to misinformation/disinformation campaigns. It is more effective to be proactive and publish information immediately rather than trying to counter misinformation after it has already spread. If you push back at Russia, it will pull back.

It is important, however, not to "hyperbolize" the Russian threat as another speaker noted. Russia has a Gross Domestic Product smaller than Canada. Its demographic trends are unfavourable as its population ages and declines, and its economy relies on energy exports – an extremely volatile commodity as we've seen in past weeks. Despite noting all this, the speaker also said that the "war is on" with Russia. It is pushing hard against the West and is winning the war by its actions to destabilize and discredit democracy. And the West is simply standing around while Russia does this. Russia wants to project invulnerability and power, but its power is an illusion – it's a Potemkin village, hollow and shallow. The West has fallen for the ruse and has persuaded itself that it cannot push back against Russia because that would lead to World War III. The West lets Russia act without responding.

Where is Canada in all this? One speaker noted that Canada has espoused certain values in the world – like support for international law and the sanctity of borders. But Canada has not acted to defend these values. Thus when Russia broke longstanding international law prohibiting the forceful change of international borders when it took Crimea, Canada (and the West) reacted only mildly. This illustrates that Canada (and the West) seems willing to compromise on basic principles. Russia acts as if it considers that only great powers are sovereign – as does China – and this is contrary to international law. This is a greater threat to Canada than Russia's weapons.

When asked about the Arctic and Russia, the responses were that the infrastructure and defensive systems there need to be updated. NORAD needs to rethink its view of Russian actions in the North. After the Cold War, NORAD was left to atrophy so now it needs to refocus on infrastructure, fuel supplies, search and rescue, and logistics in the Arctic – as Russia has been doing. As well, NORAD is attempting to evolve to deal with cyber-threats, but thus far it is only looking at cyber-defence of *NORAD*, not cyber-defence of the continent. NORAD needs to consider defence of the continent holistically and work with other agencies, particularly in terms of sensors, command and control, and response gaps.

What can be done about Russia? The West tends to think that President Vladimir Putin is an outlier and that when he is gone, Russia will revert to being a reasonable law-abiding state. This is wishful thinking. Putin taps into deep nationalist feelings in Russia. But the process underway in Russia to change the constitution and keep Putin in power is a strategic opportunity for the West. It creates vulnerabilities that the West can use to push back. Information and transparency are the greatest fears of autocrats, and providing information to Russians about corruption and venality in the upper echelons of government may swing citizens against Putin. However, even if Putin were replaced there is no guarantee that the next leader of

Russia will be better. Whoever follows Putin may be more aggressive and less intelligent.

The panel also discussed NATO in its relations with Russia. As noted here, the importance of pushing back against Russia and countering its malign activities was raised by more than one speaker. NATO, and Western countries in general, have to counter Russian untruths with truths. This has become more challenging, however, in a time when truth is missing in the West as well! NATO must work to regain its solidarity, and stop being a “rhetorical circular firing squad” if it is to counter Russia. Russia may not physically invade the Baltics, but it will destabilize and provide misinformation about the treatment of Russian-speaking minorities there to raise the temperature and feed nationalism at home. To the question of whether the United States is a credible ally in NATO, the response was that it would respond if Russia invaded the Baltic states. The problem with this is that NATO is fairly rigid on when Article V is invoked. The article needs to be made more flexible to allow response to lower level aggression, as represented by ‘little green men’ or cyber-attacks. It would be helpful to work toward a NATO declaration that Russian *interference* – rather than attack – would be seen as triggering Article V. But, given the disarray of NATO right now, such an agreement seems unlikely. In the absence of revision to Article V, NATO states must prepare for the first wave of Russian actions, which will be disinformation, and train for their own information operations. The bottom line is that if the West truly believes in a rules-based international order, it needs to act when fundamental rules of that order are broken.

The second panel addressed great powers in the Middle East. Again, this is somewhat off the topic of how to position Canada in a world of great power plays, but interesting nonetheless. The first speaker discussed how the West, the United States in particular as the major Western player in the Middle East, has been slow to realize that terrorism is no longer the major focus in the region. In the past 10 years there have been waves of social movements – the Arab Spring in 2011, and now protests in Iran, Lebanon and Iraq. The protests are about underlying social and economic problems which have been ignored by local leaders. These problems of governance allow terrorists to capitalize on social angst and anger, and are factors in the massive population movements that have led to the resurgence of the far right in Europe.

Should these protests be encouraged by the West? One of the panelists asked if the instability in the Middle East is necessarily a bad thing. There are good reasons for civilians to rise up in protest. Most governments in the Middle East have failed their citizens. The instability in the region is a symptom of a problem, not the problem itself.

Another speaker discussed how an increasingly active citizenry and loss of faith in institutions has led to an increase of protests in the Middle East. This is also the case in the West where the loss of faith in institutions is coupled with rejection of expertise. In turn this has led to populist leaders who rule by gut feeling rather than knowledge and sow further distrust in institutions and processes. Certain segments of the population become emboldened by populist leaders, and leaders are in turn emboldened to ignore complexity, and do not even try to understand or explain global situations. They simplify the world for their citizens, and citizens like this. An emboldened but ignorant citizenry is easily led. It was not made clear exactly how this relates to the Middle East, but it can be extrapolated that the United States has abandoned the Middle East based on a lack of understanding on the part of leaders, and wishful thinking on the part of American citizens. The United States has conducted one-off actions (eg., targeted assassinations and sanctions) but has no strategy or long-term plan for the region. Sanctions are a tool, not a strategy.

This illustrates a fundamental problem. Despite being there for many years, the United States does not understand the Middle East. Its pressure on Iran, for example, will not stop Iranian actions in other states, and staying out of Syria has not been a solution. In the absence of the United States in Syria, there has been a vacuum that other actors have been quick to fill – Russia, Iran, Turkey in particular. The United States has influence and strength, it is just not using it. As the speaker said, “the United States is 10 feet tall but it operates as if it is 2 feet tall.” In Syria, President Assad may win the war with Russian and Iranian assistance but he cannot win the peace with their assistance. Assad will not be able to hold the territory he regains, and the Syrian state is now in hock to Russia and Iran, as well as to a multitude of militias and rapacious non-state actors. Neither Russia nor Iran can afford to re-build the country they've done so much to destroy. The United States will eventually have to act – and this will be more difficult than if it had acted in the first place.

This panel illustrated the confluence of both traditional and non-traditional threats, in particular the discussion of health. The situation of refugees and internally displaced populations (IDPs) in the Middle East was discussed in terms of the current COVID-19 pandemic. Because of miserable living conditions and crowding, such populations are ripe for diseases of all kinds. This will sharpen the West's unwillingness to accept them. And this means that another fundamental element of the international order will have been broken – first the sanctity of borders, and now the refugee convention written in the aftermath of the Second World War.

The Chinese Ambassador to Canada was on the panel about the Middle East. This is indicative of how other great powers are moving into the vacuum left by the United States. The ambassador's speech illustrated both China's use of soft power to win friends, and the Chinese manipulation of reality. He spoke about COVID-19 and pointed out that the virus is now under control in China so it is helping others with information and medical material. China is winning the soft-power war with its actions in response to COVID-19 in Europe. In terms of the Middle East, the ambassador noted that global peace is not possible without peace in the region, and security there can only be achieved by economic prosperity. China, he said, is working hard to promote peace through development by means of its Belt and Road Initiative. He discussed China's support for cooperation and coordination and multilateralism to solve the problems in the region and noted China's significant contribution to United Nations peacekeeping. He claimed that China respects human rights, religious freedom, follows international law, and that what the West calls internment camps for Muslims are in fact vocational training centres, from which many students have graduated and found jobs. These claims may be disputed!

The question of Iran in the Middle East was discussed by an Israeli panelist. He made three points. First he noted that Iran's proxies in the region, driven and guided by the Quds Forces, have entrenched themselves in Iraq, Lebanon and Syria, and enhanced Iran's regional power. Their attacks lend deniability to Iran. Second, the disputes in the region have become much more complex, and it is often no longer clear who is fighting whom and for what purpose. In Syria for example, there are local, regional and global forces plus a mix of radical and moderate forces. And third, he discussed terrorism and non-state actors. Terrorism is not dead, and now some terrorist groups have the capabilities of states (what he referred to as 'terror armies'). These powerful groups exist in failed states or near-failed states (such as Libya, Lebanon, Yemen) in the Middle East and North Africa. The presence of non-state actors and increasingly complicated conflicts has led to the collapse of another international norm – i.e., prohibition of the use of chemical weapons and the targeting of civilians and hospitals. Again the West has remained silent while another fundamental principle of the post-WWII world has been violated.

The third panel examined trans-Atlantic cooperation. The moderator began the panel by asking questions. What is the purpose of NATO? What is NATO's relevance to the world at large? Has US leadership of NATO changed?

The first panelist noted that NATO has been based on cooperation for many years, but it has changed. At what point will these changes affect cooperation? There are now questions about the merit of the alliance and its capability and will. It needs leadership and a new vision if it is to continue. This is not new – NATO underwent the same existential angst after the Cold War ended. But the United States is now key to the future since its commitment is in doubt and NATO has historically depended on US participation.

The second panelist noted that the United Kingdom is currently conducting a defence and security review.

Defence and security policies need to be reviewed in a changing world. There are more hostile states, more cyber-attacks including on elections, and even assassinations on British soil. He noted that there are emerging themes in the UK review that would affect the West as a whole, in particular costs and risks. For example, deterrence is focussed on conventional threats, but fighting is now on a level below this. How much do you invest to counter state-based threats, and how much to counter sub-state/non-conventional threats? Western states used to train for war-fighting, and then for counter-insurgency after 9/11, but does this need to change? There should be much more attention paid to the cyber arena, and space and information. The UK, and NATO, need to rethink how to fight. They must focus on multi-domain integration and make sure all assets can communicate securely, internally and among allies. When these questions are addressed, there will be more questions. These relate to questions of the 'sunset' and 'sunrise' of capabilities. Sunset decisions relate to what capabilities should be discontinued. These decisions are difficult to make as militaries tend to be slow-moving entities, and politicians fight to protect the industries in their constituencies. The sunrise question is about what capabilities you need for tomorrow. These are higher risk and politically difficult decisions. But because of global changes, militaries and states need to take risks in terms of capability. This is extremely difficult for Western democracies which tend to focus on the short term.

The third speaker was the Commander of US Pacific Command – an odd choice for a panel focused on trans-Atlantic relations. He focused on China and painted a very different picture than the Chinese Ambassador. China promotes its own value system, and it thus represents a long-term strategic threat to the current world system. China will replace international rules and norms – and these new rules will be made in Beijing to further China's interests. Power is more important than law in Beijing's view.

There will be competition with China but that does not necessarily mean conflict. However, the West must be prepared for conflict. There are, he said, four key things to focus on to counter China. First, the United States must harness joint forces and capability and develop technology (eg., relating to missiles, command and control and logistics). This will deter China with capabilities. Second, the United States must enhance its posture in the Indo-Pacific region. This will involve allies which will be expected to help enhance surveillance. It will also involve enhanced logistics, sustainment and increased mobility and agility in the region. Third, the United States must improve exercises for readiness and interoperability. This will increase the ability of the United States and its allies to work together. Exercises reveal capabilities which in turn enhances deterrence. And fourth, the United States must strengthen allies and partners. This will involve networking, exercises, communication and interchanges with allies in all domains. He is optimistic about the future because he thinks that the Western value system compares favourably to the Chinese.

The next speaker discussed how the West shares values and this provides strength. Canada is relearning trans-Atlantic deployments – including sustainment and logistics – after the capability was lost in the years since the end of the Cold War. Geography matters less than it once did in terms of information-warfare or cyber-warfare, but it still matters to military exercises and operations. Militaries need to learn continuously, and deployed forces have to be on constant alert, not for attack by state forces but by sub-state forces or information attacks. This increases the pressures on military leaders at the tactical level, but militaries must not forget the strategic level. Cyber-space used to be an after-thought to the main battle, but now cyber/information war is the main event. Canada and NATO need strategies and plans to deal with it, they need personnel who can understand and operate in a cyber environment, and they need to enhance training to counter misinformation. As well, Western states need to align domestically on the importance of these actions, and coordinate and communicate with each other. There are opportunities and risks arising from a changing world. NATO needs to learn how to address operations below the threshold of war.

The bottom lines on this panel were clear. The biggest threat to NATO/the West is the loss of credibility, both as an alliance and as individual states. NATO cannot succeed if its primary posture of deterrence is not credible. This relates back to information management, the West being passive/reactive in the face of Russian aggression, and lack of common understanding and assessment of threats among member states. The question of adopting Huawei 5-G communication technology also cannot be allowed to divide the alliance. But this is a complicated question that has elements relating to trust, cost, politics and sovereignty.

A speech by General Jonathan Vance closed the first day. He started by saying that we need to discuss and debate issues and changes in the security environment – and challenge prevailing thought. Without this, we can't adapt. And adapting to changes is crucial, there is no choice.

Vance argued that there is a four-part framework of military engagement: conflict prevention; conflict management; conflict termination; and conflict harm reduction. Militaries have to be ready to fight, but it's better if they don't have to. This means a focus on prevention and deterrence. If conflicts can't be prevented, they must be managed (although what this meant was not defined), usually with allies. Conflict termination involves achieving the desired end of conflict. How? For Western militaries these days this involves peace support operations, building capacity and creating long-term stability. But these require civilian participation, not just military. And Western militaries are concerned about harm reduction – i.e., harming civilians is against our values, and we need to promote reduction of harm even if it makes the fight more difficult.

Modern conflicts are challenging. This is because states often deliberately keep their tactics below the threshold of war to take advantage of gray areas of policy and ensure that other states don't respond. This is what Russia did in Crimea and eastern Ukraine, as well as in its state-sponsored cyber-activities and disinformation campaigns; it is also what China does in the South China Sea. Operations below the threshold of war are "death by a 1,000 cuts," and this demands a new response. Avoiding war is not a recipe for peace – we don't want global conflict but we don't want our values destroyed by aggressive states operating below the threshold of war. The West needs to deter and/or respond, and deterrence must be credible. Military forces need to be able to stop adversaries from contemplating force in the first place.

Western states are distracted from the main threat. Small states distract us from a focus on major powers, as do non-state actors such as terrorists and criminal organizations. As well, non-military deployments – such as responses to fires, floods and snowstorms – distract militaries from their primary missions.

Canadian forces need to be flexible and agile, and harness new technologies. Canada needs to focus more on digital warfare and information/cyber-security. This means more focus on networks, band width, information management and cyber capabilities. All militaries need the right people who are motivated and have the tools to be effective so recruitment is key. The Canadian Armed Forces need to change in terms of demographics and skills, and that means ending harmful behaviour toward women and minorities, and making personnel policies more adaptable and flexible for families. And in this, hard decisions will have to be made about budgets and capabilities as new challenges appear and new funding doesn't.

The second day of the conference switched focus (for most of the day) to procurement and personnel.

In the midst of major procurement programs, there is a tendency to focus on particular projects and to lose sight of the bigger picture, for example, sustainment of forces in the field. Part of defence procurement is to assess the level of risk and to make sure that the procurement process and results match the risk, both in terms of cost and utility of the capability. There have been complaints in Canada that the procurement process is too unwieldy and slow and there have been efforts to change this. The plan is to simplify the process, change the way that government engages with industry and keep up with technology, but also to ensure that the process remains accountable and transparent. The first speaker in this panel noted that Canada spends too much time defining things, and by the time this has been done, the situation or threat or technology has changed. A procurement program needs definition because of budgets and outputs but it cannot be too rigid or it sacrifices agility. Defence Procurement Canada was formed to address challenges in procurement. The hope is that it will allow industry to provide solutions and proposals and give the procurement process more flexibility. Canada has also developed the IDEAS program to address needs and encourage innovative solutions to military problems. This involves creating opportunities to discuss matters with academics, industry and allies.

A speaker from the US Department of Defense (DoD) noted the close collaboration between Canada and the United States on defence procurement, but also noted that we don't understand each other's needs or priorities. Her role at DoD is to refocus the lines of effort to make sure that American forces are lethal, that they never fight alone, and to reform the way DoD does business. She stressed the latter element – i.e., reforming the way DoD does business. Like Canada, the US procurement process is unwieldy and this discourages small businesses from participating and reduces the willingness to take risks in the process. Her role is to streamline decision-making and make policy more simple, accessible and directed so businesses can navigate the process more easily. She wants to bring industry into DoD. An observer might note that there are problems inherent in this strategy, as we can see from the experience of letting Boeing advise aviation officials on the safety of their own airplane!

This panel returned to the idea of cyber-security. Technology and the nature of cyber-threats change very quickly and militaries need to be agile to protect themselves. We are "at war every day" on this. The US DoD spends significant time on cyber-security and works with other US agencies like National Security Agency (NSA) and the Department of Homeland Security (DHS). But cyber-security is not just a government matter, DoD is now pushing industry to ensure cyber-security, and has begun setting up a cyber-security framework with different standards for different industries. The framework is designed to examine and assess compliance and have only certified companies do business with the military. This, of course, will add a new layer of complexity for small businesses trying to work with the military – and perhaps cancel out efforts to encourage small businesses to participate in procurement projects.

The United States has been preoccupied with the wrong things. While it has been focusing on the low-tech fight against terrorists and trying to figure out how to deal with improvised explosive devices, states like China and Russia have been focusing on technology like artificial intelligence and hypersonic weapons. The US military used to lead in developing technology but that has changed – now it's private industry and that means trying to cooperate with high-tech companies that sometimes don't want to work with government agencies. Militaries need to cooperate with universities and research institutes as well but be aware that much of China's initial work in technology was acquired via stealing it from the West or buying companies and transferring technology back to China. The United States is trying to ensure that foreign entities are not buying technology companies, and to create a 'trusted capital' fund to make sure that people who provide financing for technology development are 'clean.'

The next panel addressed questions of personnel. Getting and keeping personnel has been a real problem for militaries in recent years. Militaries are 'greedy institutions' in that they insist on service to country over self, the hours are sometimes long and unpredictable, personnel (and their families) are moved regularly, and ultimately personnel could be sent off to fight and be killed. This makes the military a challenging employer. It's important to understand why people decline to join the military and why they leave the military. Information on attrition is key to addressing it. What occupations are losing personnel? People are leaving from both high and low professions, eg., both doctors and cooks. Their decision to leave will include different factors. There may be material factors (i.e., pay and benefits, opportunities in the private sector) or relational factors (such as being made to feel useful and valued). As well, generational differences have to be taken into account in recruitment strategies – younger people may have different requirements for a job. And militaries need to address the problems of sexual (and minority group) violence and harassment in the forces. Programs such as Operation Honour to address sexual harassment, and 'Seamless Canada' to help Canadian forces to smooth the transition to another part of the country, have been developed to address personnel concerns. A key concern for recruitment is getting people with the right skills, and increasingly this means people who are comfortable with and knowledgeable about technology.

It is interesting that in the discussion about personnel, and the difficulties of recruiting and retaining them, there was no mention of unmanned technology. The US Navy, for example, has developed small to medium-sized ships which can operate without a crew. And this technology is advancing rapidly. Unmanned capabilities do not yet operate without human personnel involved – i.e., there is still a need for operators and maintenance – but they will change the personnel needs of militaries.

The next panel was focused on the question of cyber-security. Cyber is not just about information technology any more, it affects all aspects of life in both the military and civilian worlds. Cyber-threats come from a variety of sources including states, criminals, terrorists and individual hackers who do it because they can. Militaries used to be able to set up commands that focused on land, sea and air but this does not adequately encompass cyber matters which affect all domains. This means new thinking about everything and building security into everything – including software, hardware, networks and applications. And again people are important, both for their skills in technology but also because most cyber-breaches are still caused by people making mistakes, usually unintentionally. In the past cyber personnel were separated from the rest of the military, but this can no longer happen, they need to integrate and cyber-security needs to be a consideration of every element of the military.

What does winning the cyber-battles and cyber-war look like? What are the threats, what are the costs of the attacks, and how much do you spend to address them? These are all questions that have yet to be answered completely. Militaries need both cyber-hygiene and cyber-resilience, and to make sure that military capabilities are secure by design. Already both civilian and military agencies are receiving millions of probes per day, some of which are increasingly sophisticated and backed by states. As the American panelist, former director of US Cyberspace Operations, said, “we’re as secure as we can be until we’re not – we’re one click away from insecurity.” To address cyber-threats, Western states have to operate holistically, and incorporate cyber-security into everything. Certain sectors of society in the West have been working hard to beef up their security – militaries and banks/financial institutions for example – but, in general, other systems such as electrical systems, water/sewage systems and traffic control systems, remain vulnerable.

Which country is more of a cyber-threat, China or Russia? Russia mixes cyber-operations with psychological operations on social media, and attacks tend to be more hardware-based. Many of these attacks do not threaten the infrastructure or personnel of the West directly, but they do threaten to undermine the trust and governance of the West. Russia is also conceiving of military operations based on cyber-operations, which China is apparently not doing. But the benefit of dealing with Russia is that the West has had many years of experience of it. The West knows far less about China, and China has more depth in technology and software. As well, China has a much bigger economy than Russia and the financial ability to pursue cyber-operations, and unlike Russia it has significant economic relations with the West. China thus could represent a threat in terms of supply chains and the integrity of components. The question of 5G technology provided by Huawei was of course a question – and responses varied. Other companies provide 5G technology, including Erickson, Nokia, Samsung but Huawei is unique in that its prices are lower, it has no internal transparency, it does not respect privacy rights, and it is (probably) an agent of an unfriendly state. The challenge is to figure out how to utilize the technology in such a way that it doesn’t compromise security, and to determine how counter-productive US pressure not to use Huawei will be.

The next session focused on moving forward and how Canada can secure its national interests. In this session, there was discussion about Canadian values, what role Canada can play in the world, and what role it is playing. In general, the discussion noted that Canada is not playing the role it used to play – it took a leading role in international activity relating to human security, land mines, child soldiers, peacekeeping, but not anymore. While acknowledging the limitations of Canada, it was suggested that Canadian civilian expertise could play a much greater role internationally in capacity- and trust-building, addressing corruption, focusing on human security, and maintaining the trans-Atlantic link in a time when the United States is not interested in Europe. But Canada is trying to conduct foreign policy on the cheap because governments believe that Canadians don't care about it. This needs to change, and governments need to talk about national interests and how they are connected to international affairs.

The final panel was about the future of war. What will war and warfare look like in the future? The old policy of deterrence, the foundation of peace during the Cold War, no longer works. In cyber-attacks, attribution is extremely difficult and time-consuming. If you can't identify a perpetrator, you can't punish them. As well, the risks and the costs of cyber-attacks are low – and the rewards are high.

Technology has been changing rapidly, but the results are not as we might have envisioned them in science fiction novels. We don't have killer robots (as yet), but we nonetheless have experienced profound changes that most people might not even notice. Computers are now present in everything, and we have the Internet of Things to link electronic devices together. It's likely that future technology will not create tools that humans use but rather will replace them in their work and war. This raises multiple legal and ethical questions. Law and policy often lag far behind the development of technology. Autocracies have an advantage in that they do not need to worry about violating citizen rights or privacy and are not limited by the law. It is difficult for liberal-democracies to undertake offensive cyber-operations because democracies are more transparent and are ruled by law.

New technology introduces new vulnerabilities that we may not understand yet. And since most citizens don't understand the technology, they focus on the wrong things about it. The new communications technologies are associated with new ideologies and new extremism. Misinformation spread via social media has led to distrust among citizens. Deep fakes created by technology will make it much more difficult to differentiate truth from lies, and this will further reduce trust in public figures. Attempting to counter malignant actors on social media has led to them making the transition to the Dark Web which is much less transparent. There are both good and bad elements to this transition. It's good in that on the Dark Web the reach is more limited, and it's bad because bad actors are much harder to catch.

The new focus of major states is artificial intelligence (AI), and there is state competition in the race to develop it. Is it an arms race? Not exactly. The difference between AI and an arms race is that individuals cannot afford aircraft carriers and missiles while AI will affect everyone. Artificial intelligence will lead to amazing new capabilities, but it also will cause unexpected problems. We still don't understand how AI comes up with solutions – the 'black box problem' – and the solutions can be surprising and problematic.

How do we mitigate the threats associated with an uncertain future and technology? Democracies need to coordinate more in their response to election interference. In particular the West can react and punish Russia in a way that hurts – for example by using information to illustrate to Russians the corruption of the Putin government. As well, democracies should put more emphasis on digital literacy to help citizens identify mis/disinformation. In addition, we have to be creative in countering mis/disinformation – for example, Al Capone was eventually convicted for mail fraud! But there is no silver bullet to fix the downsides of technology. It will be a constant struggle to manage the risks.

Conclusions

This conference has a long history – indeed it was first held in 1932. It would be fascinating to see how the focus has changed over the years. But from this year's conference we can make a number of observations. First, it was interesting that the discussion did not focus on traditional warfare or traditional roles for the military. This reflects that the non-traditional roles of the military are ascendant. The discussion ranged from cyber-security to information operations to personnel recruitment but there was virtually no discussion about fighting wars as they existed in the past. What does this mean for militaries? Their primary mission is now, as it always has been, to fight wars if they become necessary. How has this changed?

Second, it became very clear from the discussion that addressing cyber-security is key. Cyber is no longer a side issue in the conduct of warfare – it is *the* issue, and it is not just the job of militaries to ensure cyber-security. Matters relating to cyber-security/defence will be present in all elements of militaries from recruitment to procurement to fighting.

Third, China deserves more attention. Why was there no panel focusing on China? There were two panels with an Atlantic focus, no panel on China. Two panelists talked about China, one in the panel on the Middle East and one in the panel on trans-Atlantic relations, but there was no direct focus on China's roughing and interference in the world. Yes, Russia is causing problems and the trans-Atlantic relationship is in disarray, but what about China? Russia is a small player in the great global competition – China is the player that matters. If the conference was examining roughing and interference in great power plays, then surely China should be a major focus. As well, if the plan for the conference was to discuss Canada in great power plays, it would have been interesting to hear a discussion on how Canada can navigate between its two biggest trading partners, both of which are flexing their muscles in ways contrary to Canadian interests.

Fourth, a number of panelists mentioned the importance of pushing back against Russia. They suggested that Russia's disruptive behaviour should be dealt with more forcefully, and that if challenged Russia would pull back. We won't know if this is the case until we try it, but what is clearly not working is the current strategy that simply reacts to Russian actions.

Fifth, in the discussion on the first day it became clear that the values that have been so publicly proclaimed by Canada (and the West) since the Second World War – inviolable borders, sanctuary for refugees and the laws of armed conflict – are no longer emphasized. If, indeed Canada is defined by its values, as a panel on the second day of the conference argued, then Canadian values have changed. If the conference had focused on how Canada could position itself among great powers, we might have seen that Canada no longer has the luxury of loudly espousing its values, and that economic interests seem to trump values in this new world.

Sixth, and this criticism is probably not fair, but discussion of the security and defence effects of pandemics would have been interesting. This conference report is being written two weeks after the conference and in the space of only two weeks, our heads are spinning with the changes to our lives. Indeed, this conference just managed to sneak in under the wire – only a few weeks later, there are no conferences, little travel and the venue for the conference, the Chateau Laurier, is closed. The repercussions of the coronavirus will be felt for years on personal, political and economic levels. We did not realize how quickly things could change in Canada and that's a problem – panelists argued forcefully for an enhanced effort to address cyber-threats, but we also need to get better at planning and preparing for other threats. I suspect that next year's conference will have a panel on pandemics!

And two small final observations. The conference organizers deserve much credit for a job well done, and in particular for the number of women who were speakers. In the past, the vast majority of speakers at security and defence conferences were men – it was refreshing to see so many women, and to hear their excellent presentations. Finally, as an attendee representing the Naval Association of Canada, it was interesting that there was no mention of navies. But that is not surprising. A two-day conference cannot discuss everything.

Dr. Ann Griffiths received her BA (Hons) from Queen's University, her MA from the University of Calgary and her PhD from Dalhousie University, all in Political Science. For many years she was at the Centre for Foreign Policy Studies and taught Political Science at Dalhousie University. She is the Editor of Canadian Naval Review and the Coordinator of the Public Affairs Program for the Naval Association of Canada.